```
File 348:EUROPEAN PATENTS 1978-2003/Apr W04
         (c) 2003 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20030515,UT=20030508
         (c) 2003 WIPO/Univentio
? ds

Set     Items   Description
S1     196167   KEY OR CIPHER??? ? OR CYPHER??? ? OR ALGORITHM??? ?
S2       5347   (SESSION? ? OR SUBSESSION? OR DATA OR CATEGORY OR ONE()TIM-
             E)(1W)S1
S3       9583   (PUBLIC OR TWO)(1W)S1 OR TWO()KEY? ? OR KEY()PAIR? ?
S4        593   ASYMMETRIC(1W)S1
S5       2383   (MASTER OR GROUP OR COMMON)(1W)S1
S6       4639   S2(5N)(DATA OR INFORMATION OR PACKET? ? OR MESSAGE? ? OR F-
             ILE OR FILES OR CONTENT)
S7         83   S2(S)S3:S4(S)S5
S8        669   S2(20N)S3:S4
S9         61   S8(S)S5
S10        12   S7/TI,AB,CM
S11      5099   IC='H04L-009'
S12        10   S7(S)S4
S13       219   S2(3N)(COPY??? ? OR COPIE? ? OR DUPLICAT? OR REPLICAT? OR -
             REPRODUC????? ? OR FACSIMILE? OR MIRROR? ? OR CLONE? ? OR CLO-
             NING? OR VERSION? ?)
S14         4   S7(S)S13
S15        10   S13(20N)S5
S16        29   S10 OR S12 OR S14:S15
S17        29   IDPAT (sorted in duplicate/non-duplicate order)
S18        29   IDPAT (primary/non-duplicate records only)
? t18/5,k/all

 18/5,K/1     (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2003 European Patent Office. All rts. reserv.

01552360
```
Information-processing with cryptographic processing
Informationsverarbeitung mit Verschlusselungsverarbeitung
Traitement des informations avec traitement cryptographique

PATENT ASSIGNEE:
  SONY CORPORATION, (214021), 7-35 Kitashinagawa 6-chome Shinagawa-ku,
    Tokyo 141, (JP), (Applicant designated States: all)
INVENTOR:
  Asano, Tomoyuki, c/o Sony Corporation, 6-7-35 Kitashinagawa, Shinagawa-ku
    , Tokyo 141, (JP)
  Muramatsu, Katsumi, c/o Sony Corporation, 6-7-35 Kitashinagawa,
    Shinagawa-ku, Tokyo 141, (JP)
LEGAL REPRESENTATIVE:
  Pratt, Richard Wilson et al (46458), D. Young & Co, 21 New Fetter Lane,
    London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1291867 A2 030312 (Basic)
APPLICATION (CC, No, Date):   EP 2002255309 020730;
PRIORITY (CC, No, Date): JP 2001239145 010807
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR;
  IE; IT; LI; LU; MC; NL; PT; SE; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G11B-020/00; H04L-009/00; G06F-001/00

ABSTRACT EP 1291867 A2
    When contents are copied or transferred from a first
  information-processing apparatus to a second information-processing
```
```

apparatus, the contents are stored onto a recording medium of the second information-processing apparatus as they are without decryption and re-encryption. In addition, the first information-processing apparatus also supplies a title-unique key to the second information-processing apparatus to be used by the second information-processing apparatus for generating a title key, which is also stored in the recording medium. In a content reproduction process carried out by the second information-processing apparatus, a title-unique key is generated from its own keys such as a master, media and LSI keys in accordance with a title-unique-key generation sequence based on the stored title key, and is used for decrypting the contents. As a result, it is possible to provide a processing configuration for efficiently performing an operation to copy contents from an information-processing apparatus to another and an operation to store distributed contents onto a recording medium of a recipient apparatus.

ABSTRACT WORD COUNT: 163

NOTE:

Figure number on first page: 16

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application: 030312 A2 Published application without search report

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200311	1434
SPEC A	(English)	200311	40420
Total word count - document A			41854
Total word count - document B			0
Total word count - documents A + B			41854

...SPECIFICATION MK stored in the memory employed in the recording & reproduction apparatus is (i+1) and **master key** MK of generation (i-2) is required for **reproducing** certain **data** , **master key** K(i-2)master is found by the recording & reproduction apparatus by applying the unidirectional...

18/5,K/2 (Item 2 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01516132

Method and apparatus for symmetric encryption/decryption of recorded data

Verfahren und Vorrichtung zur symmetrischen Verschlusselung/Entschlusselung von aufgezeichneten Daten

Methode et dispositif de cryptage/decryptage symmetrique de donnees enregistrees

PATENT ASSIGNEE:

Sony Corporation, (214031), 6-7-35 Kitashinagawa, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)

INVENTOR:

Asano, Tomoyuki, c/o Sony Corporation, 6-7-35 Kitashinagawa, Shinagawa-Ku, Tokyo 141-0001, (JP)

Ishibashi, Yoshihito, c/o Sony Corporation, 6-7-35 Kitashinagawa, Shinagawa-Ku, Tokyo 141-0001, (JP)

Shirai, Taizo, c/o Sony Corporation, 6-7-35 Kitashinagawa, Shinagawa-Ku, Tokyo 141-0001, (JP)

Akishita, Toru, c/o Sony Corporation, 6-7-35 Kitashinagawa, Shinagawa-Ku, Tokyo 141-0001, (JP)

Yoshimori, Masaharu, c/o Sony Computer Entertainment, 7-1-1 Akasaka, Minato-ku, Tokyo 107-0052, (JP)

Tanaka, Makoto, c/o Sony Computer Entertainment, 7-1-1 Akasaka, Minato-ku, Tokyo 107-0052, (JP)
LEGAL REPRESENTATIVE:
Robinson, Nigel Alexander Julian et al (69551), D. Young & Co., 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1267515 A2 021218 (Basic)
APPLICATION (CC, No, Date): EP 2002078475 010119;
PRIORITY (CC, No, Date): JP 200013322 000121; JP 200015551 000125; JP 200015858 000125; JP 200016029 000125; JP 200016213 000125; JP 200016251 000125; JP 200016292 000125
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
RELATED PARENT NUMBER(S) - PN (AN):
EP 1195734 (EP 2001901463)
INTERNATIONAL PATENT CLASS: H04L-009/06; H04L-009/32

ABSTRACT EP 1267515 A2
A record reproducing player and save data processing methods capable of insuring security of save data are provided. Save data is stored in a recording device, encrypted with the use of a program's individual encryption key, e.g., a content key, or a save data encryption key created based the content key, and when reproducing the save data a decryption process is conducted on it with the use of the save data decryption key particular to the program. Furthermore, it is made possible to create save data encryption keys based on a variety of restriction information, such as performing the storing and reproducing of the save data by conducting encryption and decryption on the save data with the save data encryption keys and decryption keys created with the use of a record reproducing player's individual key or a user's password.
ABSTRACT WORD COUNT: 140
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	021218 A2	Published application without search report
Assignee:	030108 A2	Transfer of rights to new applicant: Sony Computer Entertainment Inc. (3064090) 7-1-1 Akasaka, Minato-ku Tokyo 107-0052 JP Sony Corporation (214031) 6-7-35 Kitashinagawa, Shinagawa-ku Tokyo 141-0001 JP
Change:	030305 A2	Inventor information changed: 20030114

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200251	6596
SPEC A	(English)	200251	73431
Total word count - document A			80027
Total word count - document B			0
Total word count - documents A + B			80027

...SPECIFICATION owned by the individual that has issued the public key, the document encrypted with the **public key** can be decrypted only by individuals having the secret key. A representative **public key** cryptosystem is the RSA (Rivest-Shamir-Adleman) encryption.
The use of such a cryptosystem enables...

...using a content decrypting key, that is, the decryption key in order to obtain and **reproduce** decrypted **data** from the encrypted data.
According to the conventional example of configuration shown in Fig. 1 ...an apparatus-specific key, which is specific to a data processing apparatus and a system **common key** , which is common to other **data**

processing apparatuses.

Furthermore, here is encryption processing of content data as a method of limiting...according to the present invention is characterized in that the data processing apparatus has a **common** signature **key** common to all entities of a system for executing a data verifying process and an apparatus-specific signature **key** specific to each apparatus that executes a data verifying process.

Further, one embodiment of the...check value, the collation is not established, control is executed such as to suspend the **reproduction** process executed in the **reproduction** process section.

Further, one embodiment of the data processing method according to the present invention...individual keys necessary to execute the encryption processing based on the master keys and identification **data** of the apparatus or data subject to encryption processing.

According to another embodiment of the...

...medium or communication medium, characterized in that the storage section stores a distribution key generation **master key** MKdis for generating a distribution key Kdis used for encryption processing of the transfer data and the encryption processing section executes encryption processing based on the distribution key generation **master key** MKdis stored in the storage section and a data identifier, which is identification data of the transfer data and generates the transfer **data** distribution **key** Kdis.

Furthermore, according to another embodiment of the data processing apparatus of the present invention...generation processing that generates an individual key necessary to execute encryption processing based on the **master key** and identification data of the apparatus or **data** subject to encryption processing is encryption processing that uses at least part of identification data...

...encryption processing on the contents data, and the contents data utilization apparatus generates a contents **data** distribution **key** based on the distribution key generation **master key** and contents identifier, which is an identifier of supplied contents data and executes decryption processing...

18/5,K/3 (Item 3 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01504244

DATA ACCESS MANAGEMENT SYSTEM AND MANAGEMENT METHOD USING ACCESS CONTROL TICKET

DATENZUGRIFFSMANAGEMENTSYSTEM UND MANAGEMENTVERFAHREN MIT EINEM ZUGRIFFSSTEUERTICKET

SYSTEME DE GESTION D'ACCES AUX DONNEES ET PROCEDE DE GESTION UTILISANT UN BILLET DE COMMANDE D'ACCES

PATENT ASSIGNEE:

Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)

INVENTOR:

YOSHINO, Kenji, c/o Sony Corporation, 7-35, Kitashinagawa 6-Chome, Shinagawa-Ku, Tokyo 141-0001, (JP)

Ishibashi, Yoshihito, c/o Sony Corporation, 7-35, K itashinagawa 6-Chome, Shinagawa-Ku, Tokyo 141-0001, (JP)

SHIRAI, Taizo, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-Chome, Shinagawa-Ku, Tokyo 141-0001, (JP)

TAKADA, Masayuki, c/o Sony Corporation, 7-35, Kitashinagawa 6-Chome,

Shinagawa-Ku, Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
Robinson, Nigel Alexander Julian et al (69551), D. Young & Co., 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1303075 A1 030416 (Basic)
WO 2002076013 020926
APPLICATION (CC, No, Date): EP 2002702791 020307; WO 2002JP2113 020307
PRIORITY (CC, No, Date): JP 200173353 010315
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/00; G09C-001/00; G06F-012/14; G06F-015/00; G06F-017/60; G06F-019/00; G06F-017/00; G06K-019/00

ABSTRACT EP 1303075 A1
To provide a data access management system that enables access control management for data files stored in a memory of a device. The system manages data access processing performed by an access unit for a memory-loaded device, and issues a service permission ticket (SPT), which serves as an access control ticket in which an access mode to be accepted for the access unit, such as a reader/writer, is set. The memory-loaded device receives the service permission ticket (SPT) from the access unit, and performs processing according to the access mode indicated in the service permission ticket (SPT). The service permission tickets (SPTs) in which access modes to be accepted for the access units are set are individually issued according to the access units. Accordingly, various modes of access according to the access units can be executed.
ABSTRACT WORD COUNT: 137
NOTE:
Figure number on first page: 0001

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	021120	A1	International application. (Art. 158(1))
Application:	021120	A1	International application entering European phase
Application:	030416	A1	Published application with search report
Examination:	030416	A1	Date of request for examination: 20021031

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200316	8394
SPEC A	(English)	200316	79434
Total word count - document A			87828
Total word count - document B			0
Total word count - documents A + B			87828

...SPECIFICATION processing using a service permission ticket (SPT) in the system of the present invention when **common** -key authentication and **common - key** ticket verification are performed.
Fig. 92 is a diagram illustrating file access processing using a...

...Partition Manager Configuration
A5. Ticket User (Reader/Writer as Device Access Unit) Configuration
A6. Public **Key** Certificate
A7. Storage Data in Device Memory
A7.1. Device-Unique-Information/Device-Partition- Information...

...Device Manager Management Processing
B3.1. Device Registration processing by Device Manager
B3.2. Public **Key** Certificate Issuing Processing under Device Manager Control

, or **common - key** authentication information and a **session key** , which are obtained by the partition authentication or the device authentication executed with said access...

...according to claim 88, wherein said memory-loaded device generates an authentication table in which **public - key** authentication information and a **session key** , or **common - key** authentication information and a **session key** , which are obtained by the partition authentication or the device authentication executed with said access...

18/5,K/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01504243
MEMORY ACCESS CONTROL SYSTEM AND MANAGEMENT METHOD USING ACCESS CONTROL TICKET
VORRICHTUNG ZUR SPEICHERZUGRIFFSTEUERUNG UND VERWALTUNGSVERFAHREN UNTER VERWENDUNG EINES SPEICHERZUGRIFFSTICKETS
SYSTEME DE CONTROLE D'ACCES A LA MEMOIRE ET PROCEDE DE GESTION FAISANT APPEL A UN TICKET DE CONTROLE D'ACCES
PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
YOSHINO, Kenji, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome,Shinagawa-ku,, Tokyo 141-0001, (JP)
ISHIBASHI, Yoshihito, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome,Shinagawa-ku,, Tokyo 141-0001, (JP)
SHIRAI, Taizo, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome,Shinagawa-ku,, Tokyo 141-0001, (JP)
TAKADA, Masayuki, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome,Shinagawa-ku,, Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
Mills, Julia et al (97061), D Young & Co, 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1276271 A1 030115 (Basic)
WO 2002076012 020926
APPLICATION (CC, No, Date): EP 2002702790 020307; WO 2002JP2112 020307
PRIORITY (CC, No, Date): JP 200173352 010315
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/00; G09C-001/00; G06F-012/14; G06F-015/00; G06F-017/60; G06F-019/00; G06K-017/00; G06K-019/00

ABSTRACT EP 1276271 A1
To provide a memory access control system in which partitions, which are divided memory areas generated in a device, can be independently managed. In response to access to the divided memory areas, which are a plurality of partitions, various types of access control tickets are issued under the management of each device or partition manager, and processing based on rules indicated in each ticket is performed in a memory-loaded device. A memory has a partition, which serves as a memory area managed by the partition manager, and a device manager management area managed by the device manager. Accordingly, partition authentication and device authentication can be executed according to either a public-key designation method or a common-key designation method.

ABSTRACT WORD COUNT: 119
NOTE:
  Figure number on first page: 0001

LEGAL STATUS (Type, Pub Date, Kind, Text):
 Application: 021120 A1 International application. (Art. 158(1))
 Application: 021120 A1 International application entering European
                            phase
 Application: 030115 A1 Published application with search report
 Examination: 030115 A1 Date of request for examination: 20021111
LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:
Available Text Language   Update   Word Count
      CLAIMS A (English) 200303   3051
      SPEC A   (English) 200303   73024
Total word count - document A   76075
Total word count - document B   0
Total word count - documents A + B   76075

...SPECIFICATION processing using a service permission ticket (SPT) in the
  system of the present invention when **common - key** authentication and
  common - key ticket verification are performed.
     Fig. 92 is a diagram illustrating file access processing using a
  service permission ticket (SPT) in the system of the present invention
  when **common - key** authentication and public- **key** ticket verification
  are performed.
     Fig. 93 is a flowchart illustrating data updating processing using a
  ...

18/5,K/5   (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01330100
DATA AUTHENTICATION SYSTEM
DATEN-IDENTIFIZIERUNGS-SYSTEM
SYSTEME D'AUTHENTIFICATION DE DONNEES
PATENT ASSIGNEE:
  Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku,
    Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
  ASANO, Tomoyuki, Sony Corporation, 7-35, Kitashinagawa 6-chome,
    Shinagawa-ku, Tokyo 141-0001, (JP)
  ISHIBASHI, Yoshihito, Sony Corporation, 7-35, Kitashinagawa 6-chome,
    Shinagawa-ku, Tokyo 141-0001, (JP)
  SHIRAI, Taizo, Sony Corporation, 7-35, Kitashinagawa 6-chome,
    Shinagawa-ku, Tokyo 141-0001, (JP)
  AKISHITA, Toru, Sony Corporation, 7-35, Kitashinagawa 6-chome,
    Shinagawa-ku, Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
  Robinson, Nigel Alexander Julian et al (69551), D. Young & Co., 21 New
    Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1195734 A1 020410 (Basic)
                              WO 200154099 010726
APPLICATION (CC, No, Date):   EP 2001901463 010119; WO 2001JP346 010119
PRIORITY (CC, No, Date): JP 200013322 000121; JP 200015551 000125; JP
    200015858 000125; JP 200016029 000125; JP 200016213 000125; JP
    200016251 000125; JP 200016292 000125
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;
  LU; MC; NL; PT; SE; TR

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
RELATED DIVISIONAL NUMBER(S) - PN (AN):
(EP 2002078475)
INTERNATIONAL PATENT CLASS: G09C-001/00; H04L-009/32

ABSTRACT EP 1195734 A1
A data processing apparatus a data processing method efficiently ascertain that data are valid, prevent encryption processing key data from leaking, eliminate illegal use of contents data, restrict contents utilization, apply a different plurality of data formats to contents and efficiently execute reproduction processing of compressed data. The verification process of partial data is executed by collating the integrity partial data as check values for a combination of partial data of a content, and the verification process of the entirety of the combination of partial data is executed by collating partial-integrity-check-value-verifying integrity check values that verify the combination of the partial integrity check values. Master keys to generate individual keys necessary for a process of such as data encryption are stored in the storage section and keys are generated as required. An illegal device list is stored in the header information of a content and referred to when data is used. Keys specific to a data processing apparatus and common keys are stored and the keys are selectively used according to the content use restriction. Plural content blocks are coupled, and at least a part of the content blocks is applied to an encryption process by an encryption key Kcon, then encryption key data that is the encryption key Kcon encrypted by an encryption key Kdis is stored in the header section. A content data is made of compression data and an expansion processing program or a combination of types of compression programs and the reproducing apparatus can determine an expansion program applicable to a compressed content.
ABSTRACT WORD COUNT: 258
NOTE:
Figure number on first page: 28

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	010919	A1	International application. (Art. 158(1))
Application:	010919	A1	International application entering European phase
Application:	020410	A1	Published application with search report
Examination:	020410	A1	Date of request for examination: 20011026
Change:	021016	A1	Application number of divisional application (Article 76) changed: 20020829

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200215	13797
SPEC A	(English)	200215	73409
Total word count - document A			87206
Total word count - document B			0
Total word count - documents A + B			87206

...SPECIFICATION means 20, the user obtains encrypted data from the storage means 20 and causes the **reproduction** process section 14 of the reproduction means 10 to execute the decryption process using a the original content data will be possible, so that a large number of **copied** content **data** available to information apparatuses such as game apparatuses or PCs may be created or tampered...arithmetic operation process on decrypted data obtained by decrypting the encrypted data, executes a signature **key** -applied cryptography process on data on arithmetic operation results obtained by the arithmetic operation, to... data and the encryption processing section executes encryption processing

based on the distribution key generation **master key** MKdis stored in the storage section and a data identifier, which is identification data of the transfer data and generates the transfer **data** distribution **key** Kdis.

Furthermore, according to another embodiment of the data processing apparatus of the present invention...aspect of the present invention is a data processing system configured by a plurality of **data** processing apparatuses, characterized in that each of the plurality of data processing apparatuses has a **common** master key to generate a key used for encryption processing of at least one of data encryption...

...processing and signature processing and each of the plurality of data processing apparatuses generates a **common** individual **key** necessary to execute the encryption processing based on the **master key** and identification data of the apparatus or data subject to encryption processing.

Furthermore, according to...

...the contents data providing apparatus and contents data utilization apparatus have a distribution key generation **master key** to generate a contents **data** distribution **key** used for encryption processing of circulation contents data between the contents data providing apparatus and contents data utilization apparatus, the contents data providing apparatus generates a contents **data** distribution **key** based on the distribution key generation **master key** and contents identifier, which is an identifier of supplied contents data and executes encryption processing on the contents data, and the contents data utilization apparatus generates a contents **data** distribution **key** based on the distribution **key** generation **master key** and contents identifier, which is an identifier of supplied contents data and executes decryption processing...utilizes the contents data, characterized in that the contents data providing apparatus generates a contents **data** distribution **key** based on a distribution key generation **master key** for generating a contents **data** distribution **key** used for encryption processing on contents data and a contents identifier, which is the identifier...

...encryption processing on the contents data, and the contents data utilization apparatus generates a contents **data** distribution **key** based on the distribution key generation **master key** and a contents identifier, which is the identifier of the provided contents data and executes...

...data processing apparatus A, a step of generating the same contents key as the contents **key** by different data processing apparatus B based on the same the contents key generation **master** key as that of the **data** processing apparatus A and the apparatus identifier of the data processing apparatus A, and a...executed by the encryption processing section.

A fifteenth aspect of the present invention is a **data** processing method that processes contents data supplied from a storage medium or communication medium, comprising...

...comprises a step of executing encryption processing applying an illegal device list check value generation **key** to illegal device list configuration data to be verified and generating illegal device list check...contents data, a control section that executes control over the encryption processing section, a system **common key** used for encryption processing in the encryption processing section, which is common to other data...

other data processing apparatuses using the contents data or an apparatus-specific key...processing configuration in CBC mode of the encryption processing section is a configuration in which **common key** encryption processing is applied a plurality of times only to part of a message string...the present invention is characterized in that in the decryption processing configuration in CBC mode, **common key** encryption processing is applied a plurality of times only to part of a message string...

...characterized in that the encryption processing configuration in CBC mode is a configuration in which **common key** encryption processing is applied a plurality of times only to part of a message string...an apparatus-specific key, which is specific to the data processing apparatus and a system **common key** , which is common to other data processing apparatuses using contents data, making it possible to process contents according to contents utilization restrictions. The data processing apparatus selectively uses these **two keys** according to contents utilization restrictions. For example, in the case where the contents are only...

...value for the contents data is generated and collation processing is performed using the system **common key** . It is possible to decrypt and reproduce the encrypted data only when the collation is...

18/5,K/6 (Item 6 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01307658
Broadcasting encrypted messages using session keys
Verteilung von verschlusselten Nachrichten unter Verwendung von Sitzungsschlusseln
Diffusion de messages chiffres utilisant des cles de session
PATENT ASSIGNEE:
Research In Motion Limited, (1900501), 295 Phillip Street, Waterloo, Ontario N2L 3W8, (CA), (Applicant designated States: all)
INVENTOR:
Little, Herb A., 523A Rosemeadow Crescent, Waterloo, Ontario N2T 1Z9, (CA)
Hind, Hugh R., 41 Dawson Crescent, Georgetown, Ontario L7G 1H3, (CA)
LEGAL REPRESENTATIVE:
Winter, Brandl, Furniss, Hubner, Ross, Kaiser, Polte Partnerschaft (100051), Patent- und Rechtsanwaltskanzlei Alois-Steinecker-Strasse 22, 85354 Freising, (DE)
PATENT (CC, No, Kind, Date): EP 1119132 A2 010725 (Basic)
EP 1119132 A3 030102
APPLICATION (CC, No, Date): EP 2001101074 010118;
PRIORITY (CC, No, Date): US 487863 000119
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/08

ABSTRACT EP 1119132 A2
A system and method for sending encrypted information to multiple recipients is provided. Information such as a message or data to be sent to multiple recipients is encrypted using a selected session key, thereby generating a first encrypted message. The session key is then encrypted with each of a plurality of unique secrets respectively associated with

the multiple recipients to thereby generate a plurality of encrypted session keys. The encrypted message and the plurality of encrypted session keys are combined in a second encrypted message, which is transmitted to the multiple recipients. Each of the multiple recipients searches the encrypted message for an encrypted session key which was encrypted with its associated unique secret, decrypts the encrypted session key to retrieve the session key and decrypts an encrypted message using the retrieved session key.

ABSTRACT WORD COUNT: 135

NOTE:

Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	010725	A2 Published application without search report
Examination:	010725	A2 Date of request for examination: 20010216
Search Report:	030102	A3 Separate publication of the search report

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200130	2039
SPEC A	(English)	200130	3926
Total word count - document A			5965
Total word count - document B			0
Total word count - documents A + B			5965

...SPECIFICATION customers would be able to acquire the session key by monitoring the list of encrypted **versions** of the **session key** , identifying the **version** encrypted using their **master key** , then decrypting the value. Hence, the show could then be broadcast once in encrypted form...the encrypted message. A suitable identifier is required so that the recipient can identify which **version** of the **session key** should be decrypted with its **master key** .

The present invention also works when used with a public key scheme. In a public...

18/5,K/7 (Item 7 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01276898

CONTENTS MANAGEMENT SYSTEM, DEVICE, METHOD, AND PROGRAM STORAGE MEDIUM

INHALTSVERWALTUNGSSYSTEM, VORRICHTUNG, VERFAHREN UND PROGRAMMSPEICHERMEDIUM

SYSTEME, DISPOSITIF, PROCEDE ET SUPPORT DE PROGRAMME POUR LA GESTION DE CONTENUS

PATENT ASSIGNEE:

Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)

INVENTOR:

ISHIBASHI, Yoshihito, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)

OHISHI, Tateo, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)

MUTO, Akihiro, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)

KITAHARA, Jun, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)

SHIRAI, Taizou, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)

LEGAL REPRESENTATIVE:

DeVile, Jonathan Mark, Dr. et al (91151), D. Young & Co 21 New Fetter

Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1128598 A1 010829 (Basic)
WO 200119017 010315
APPLICATION (CC, No, Date): EP 2000956997 000907; WO 2000JP6089 000907
PRIORITY (CC, No, Date): JP 99253660 990907; JP 99253661 990907; JP 99253662 990907; JP 99253663 990907; JP 99260638 990914; JP 99264082 990917; JP 99265866 990920
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/32; G06F-015/00; H04N-005/91; G11B-020/10; G10K-015/04; H04N-007/167
CITED REFERENCES (WO A):
JP 8305662 A
JP 8185444 A
WO 9909718 A1
JP 2041051 A
JP 11185381 A
JP 7182837 A
WO 9627155 A3
KINEO MATSUI: 'Internet saishin technology: The 13rd digital contents no chiteki shoyuuken wo mamoru denshi sukashi' INTERNET MAGAZINE no. 37, 1998, pages 352 - 355
FUMITADA TAKAHASHI: 'Digital shingou shori: 'Denshi sukashi' ga multimedia jidai wo mamoru; Chosakuken hogo gijutsu no yuuryoku kouho; Chosakubutsu no fusei riyou boushi ni myoushu ari: Denshi sukashi de copy wo yokusei' NIKKEI ELECTRONICS no. 683, 1997, pages 99 - 107
ASANO: 'Technology ga ippai; Digital contents wo mamoru digital sukashi' ASCII vol. 21, no. 9, 1997, pages 210 - 215
TARO YOSHIO: 'Kogata memory card de ongaku chosakuken wo mamoru' NIKKEI ELECTRONICS no. 739, 22 March 1999, pages 49 - 53
FUMITADA TAKAHASHI, TARO YOSHIO: 'Ongaku haishin mattanashi; Seibi isogu chosakuken hogo gijutsu sasaeru gijutsu jitsuyouki no haishin system; chosakuken kanti ga kagi nigiru' NIKKEI ELECTRONICS no. 738, 08 March 1999, pages 94 - 98
TETSUO NAKAGAWA ET AL.: 'Digital contents ryuutsu gijutsu' MITSUBISHI DENKI GIHOU vol. 72, no. 5, 1998, pages 36 - 39
SHOKO MOTOIKE, MASAKI KIYONO: 'DVD wo mochiita contents ryuutsu service' MATSUSHITA TECHNICAL JOURNAL vol. 44, no. 5, 1998, pages 25 - 33
NAOJI USUKI ET AL.: '5C Digital transmission content protection; IEEE1394 bus no chosakuken hogo houshiki' EIZOU MEDIA GAKKAI GIJUTSU HOUHOKU vol. 22, no. 65, 1998, pages 37 - 42 (CE'98-14)
DAISUKE IMAIZUMI: 'Ongaku haishin souchi to shiteno internet' COMPUTOPIA vol. 34, no. 393, 01 June 1999, pages 96 - 97
DIGITAL TRANSMISSION CONTENT PROTECTION SPECIFICATION, REVISION 1.0, INFORMATIONAL VERSION 12 April 1999,
HIRONOBU YAMAMOTO ET AL.: 'Chosakuken wo hogo shita ongaku haishin platform' NTT R&D vol. 48, no. 10, 10 October 1999, pages 762 - 769;

ABSTRACT EP 1128598 A1
An information receiving apparatus receives identification information and encrypted identification information and makes a comparison between them to allow prevention of illegal utilization of contents data. Also, a data storage apparatus can record contents data encrypted by a content key and the content key so that the contents data can be reproduced on other apparatuses to improve versatility. Moreover, a management apparatus can manage the contents data in the data storage apparatus to allow other apparatuses to utilize it. And also, an information regulating apparatus can verify a signature on available data to prevent illegal utilization of the contents data. Furthermore, the data storage apparatus can store the content key, its handling policies, the contents data encrypted by the content key and its license conditions information

so as to safely provide the contents data. In addition, an information recording apparatus can select favorite contents data and store it on the data storage apparatus. Furthermore, the information receiving apparatus can prevent utilization of provision-prohibited contents data by a provision prohibition list.

ABSTRACT WORD COUNT: 172

NOTE:

Figure number on first page: 0020

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	010509	A1 International application. (Art. 158(1))
Application:	010509	A1 International application entering European phase
Application:	010829	A1 Published application with search report
Examination:	010829	A1 Date of request for examination: 20010502

LANGUAGE (Publication,Procedural,Application): English; English; Japanese

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200135	29406
SPEC A	(English)	200135	83907
Total word count - document A			113313
Total word count - document B			0
Total word count - documents A + B			113313

...SPECIFICATION a content key by a save key, recording a content key encrypted by a save **key** and the contents data encrypted by the content key on a record medium or reproducing...data received by an information receiving apparatus will be illicitly utilized and preventing the contents **data** from being illicitly utilized.

Also, in the present invention, an information regulating apparatus connected online...

...illegal data and if determined so, prohibiting the information receiving apparatus from utilizing the contents **data** by information regulating apparatus.

Thus, an information provision method can be implemented, which is capable...apparatus, an information provision method and a program storage medium capable of easily providing contents **data** can be implemented.

In addition, the present invention provides, in an data storage apparatus storing predetermined contents **data** sent from an information provision apparatus, the means for receiving a content key and contents ...

...if an information user does not have a contents data receiving apparatus, to record contents **data** with ensured security, and accordingly a data storage apparatus, a data storage method and a...block diagram showing data contents of the equipment.

Figure 19 is a block diagram showing **data** contents held by a record medium.

Figure 20 is a skeleton ...symmetrical key technology.

Figure 52 is a timing chart showing a mutual authentication process using **asymmetrical key** technology.

Figure 53 is a skeleton block diagram showing transmitting operation of accounting information.

Figure...

18/5,K/8 (Item 8 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

00690802

Apparatus for implementing a symmetric block ciphering algorithm without the complementation property

Vorrichtung zur Durchfuhrung eines symmetrischen Blockchiffrierungsalgorithmus ohne die Eigenschaft der Komplementierung

Appareil de mise en oeuvre de l'algorithme de chiffrage symetrique par bloc sans la propriete de complementation

PATENT ASSIGNEE:
GENERAL INSTRUMENT CORPORATION, (2532982), 101 Tournament Drive, Horsham, PA 19044, (US), (Proprietor designated states: all)
INVENTOR:
Sprunk, Eric, 2948 Corte Diana, Carlsbad, California 92009, (US)
LEGAL REPRESENTATIVE:
Hoeger, Stellrecht & Partner (100381), Uhlandstrasse 14 c, 70182 Stuttgart, (DE)

PATENT (CC, No, Kind, Date): EP 660563 A1 950628 (Basic)
EP 660563 B1 010228
APPLICATION (CC, No, Date): EP 94118066 941116;
PRIORITY (CC, No, Date): US 167781 931221
DESIGNATED STATES: DE; ES; FR; GB
INTERNATIONAL PATENT CLASS: H04L-009/06

CITED REFERENCES (EP B):
PROCEEDINGS OF COMPCON '78 - COMPUTER COMMUNICATIONS NETWORKS 5-8 September 1978, Washington DC (US) NEW YORK (US)
D.W.DAVIES & W.L.PRICE 'SECURITY FOR COMPUTER NETWORKS An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer' 1989 , JOHN WILEY & SONS , CHICHESTER(GB) * pages 61,64 & 65 * * page 61, line 41 - page 65, line 9 *;

ABSTRACT EP 660563 A1

An implementation of a security algorithm such as DES is provided that overcomes the complementarity weaknesses provided by conventional implementations. In a DES implementation, a cryptographic processor (10) applies the DES algorithm to a data block. The DES processor includes a first input port (14) for receiving the data block (X), a second input port (12) for receiving a cryptographic key (K), and an output port (15) for outputting the data block after encryption. A nonlinear function (20, 22, 24) that does not have complementarity is applied to at least one of the ports. The nonlinear function can comprise a lookup table, which could be advantageously derived from a DES S-Box. (see image in original document)

ABSTRACT WORD COUNT: 118

NOTE:
Figure number on first page: 2

LEGAL STATUS (Type, Pub Date, Kind, Text):

Examination:	000503	A1	Date of dispatch of the first examination report: 20000315
Application:	950628	A1	Published application (A1with Search Report ;A2without Search Report)
Lapse:	020626	B1	Date of lapse of European Patent in a contracting state (Country, date): ES 20010228,
Grant:	010228	B1	Granted patent
Oppn None:	020220	B1	No opposition filed: 20011129
Examination:	951227	A1	Date of filing of request for examination: 951026
*Assignee:	981007	A1	Applicant (transfer of rights) (change): GENERAL INSTRUMENT CORPORATION (2552750) 10

Melville Park Road Melville, NY 11747-3113 (US) (applicant designated states: DE;ES;FR;GB)

*Assignee: 981007 A1 Previous applicant in case of transfer of rights (change): GENERAL INSTRUMENT CORPORATION OF DELAWARE (1783080) 181 West Madison Street Chicago, Illinois 60602 (US) (applicant designated states: DE;ES;FR;GB)

*Assignee: 981014 A1 Applicant (transfer of rights) (change): GENERAL SEMICONDUCTOR, Inc. (2552760) 10 Melville Park Road Melville, NY 11747-3113 (US) (applicant designated states: DE;ES;FR;GB)

*Assignee: 981014 A1 Previous applicant in case of transfer of rights (change): GENERAL INSTRUMENT CORPORATION (2552750) 10 Melville Park Road Melville, NY 11747-3113 (US) (applicant designated states: DE;ES;FR;GB)

*Assignee: 981021 A1 Applicant (transfer of rights) (change): GENERAL INSTRUMENT CORPORATION (2532982) 101 Tournament Drive Horsham, PA 19044 (US) (applicant designated states: DE;ES;FR;GB)

*Assignee: 981021 A1 Previous applicant in case of transfer of rights (change): GENERAL SEMICONDUCTOR, Inc. (2552760) 10 Melville Park Road Melville, NY 11747-3113 (US) (applicant designated states: DE;ES;FR;GB)

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB95	502
CLAIMS B	(English)	200109	528
CLAIMS B	(German)	200109	486
CLAIMS B	(French)	200109	544
SPEC A	(English)	EPAB95	2217
SPEC B	(English)	200109	2186
Total word count - document A			2720
Total word count - document B			3744
Total word count - documents A + B			6464

...SPECIFICATION signal. Each descrambler has its unique unit key signal stored in memory for use in **reproducing** the **common category key** signal when the descrambler is addressed by its unique encrypted category key signal. By using...

...SPECIFICATION signal. Each descrambler has its unique unit key signal stored in memory for use in **reproducing** the **common category key** signal when the descrambler is addressed by its unique encrypted category key signal. By using...

18/5,K/9 (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00527049
Public key cryptosystem key management based on control vectors.
Schlusselverwaltung fur Geheimubertragungssystem mit offentlichem Schlussel auf Grundlage von Steuervektoren.
Administration de cle pour systeme cryptographique a cle publique basee sur des vecteurs de commande.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road,

Armonk, N.Y. 10504, (US), (applicant designated states:
AT;CH;DE;DK;ES;FR;GB;IT;LI;NL;SE)
INVENTOR:
Matyas, Stephen M., 10 298 Cedar Ridge Drive, Manassas, VA 22 110, (US)
Johnson, Donald B., 11 635 Crystal Creek Lane, Manassas, VA 22 111, (US)
Le, An V., 10 227 Battlefield Drive, Manassas, VA 22 110, (US)
Prymak, Rostislaw, 15 900 Fairway Drive, Dumfries, VA 22 026, (US)
Martin, William C., 1835 Hilliard Lane, Concord, NC 28 025, (US)
Rohland, William S., 4234 Rotunda Road, Charlotte, NC 28 226, (US)
Wilkins, John D., P.O. Box 8, Somerville, VA 22 739, (US)
LEGAL REPRESENTATIVE:
Schafer, Wolfgang, Dipl.-Ing. (62021), IBM Deutschland
Informationssysteme GmbH Patentwesen und Urheberrecht, D-70548
Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 534419 A2 930331 (Basic)
EP 534419 A3 940629
APPLICATION (CC, No, Date): EP 92116307 920911;
PRIORITY (CC, No, Date): US 766260 910927
DESIGNATED STATES: AT; CH; DE; DK; ES; FR; GB; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: H04L-009/08;

ABSTRACT EP 534419 A2

A data processing system, method and program are disclosed, for managing a public key cryptographic system. The method includes the steps of generating a first public key and a first private key as a first pair in the data processing system, for use with a first public key algorithm and further generating a second public key and a second private key as a second pair in the data processing system, for use with a second public key algorithm. The method then continues by assigning a private control vector for the first private key and the second private key in the data processing system, for defining permitted uses for the first and second private keys. Then the method continues by forming a private key record which includes the first private key and the second private key in the data processing system, and encrypting the private key record under a first master key expression which is a function of the private control vector. The method then forms a private key token which includes the private control vector and the private key record, and stores the private key token in the data processing system.

At a later time, the method receives a first key use request in the data processing system, requiring the first public key algorithm. In response to this, the method continues by accessing the private key token in the data processing system and checking the private control vector to determine if the private key record contains a key having permitted uses which will satisfy the first request. The method then decrypts the private key record under the first master key expression in the data processing system and extracts the first private key from the private key record. The method selects the first public key algorithm in the data processing system for the first key use request and executes the first public key algorithm in the data processing system using the first private key to perform a cryptographic operation to satisfy the first key use request. (see image in original document)
ABSTRACT WORD COUNT: 343

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	930331	A2	Published application (Alwith Search Report ;A2without Search Report)
Change:	930512	A2	Representative (change)
Examination:	930908	A2	Date of filing of request for examination: 930716
Change:	930929	A2	Representative (change)
Search Report:	940629	A3	Separate publication of the European or

International search report

Change:	940921 A2	Representative (change)
Examination:	970611 A2	Date of despatch of first examination report: 970424
Withdrawal:	990602 A2	Date on which the European patent application was deemed to be withdrawn: 981215

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	3823
SPEC A	(English)	EPABF1	40413
Total word count - document A			44236
Total word count - document B			0
Total word count - documents A + B			44236

...SPECIFICATION 728, 4,924,514, which are based on a symmetric key algorithm such as the **Data** Encryption **Algorithm** (DEA), make use of a key hierarchy wherein keys belonging to a cryptographic device are encrypted with a single **master key** and stored in a key data set. The **master key** is stored in clear form within the cryptographic hardware. The concept of using a single **master key** to encrypt keys stored in a key data set is known as the **master key** concept (see C.H. Meyer and S.M. Matyas, Cryptography--A New Dimension in Computer Data Security, John Wiley & Sons, Inc., New York, 1982.). Until now, the **master key** concept has been applied only to cryptographic systems based on a symmetric key cryptographic algorithm. However, the present invention extends the **master key** concept and teaches how it may be applied to cryptographic systems based on an **asymmetric key** cryptographic algorithm, and more particularly how it may be applied to cryptographic systems incorporating both...

...key cryptographic algorithms, generally called hybrid cryptographic systems. The reader will appreciate that in a **public key** based cryptographic system employing (1) an **asymmetric algorithm** or (2) both asymmetric and symmetric algorithms, there is still a need to use many...the set of all binary numbers of their magnitude. When the cryptographic algorithm is an **asymmetric algorithm** such as the RSA algorithm, there are **two keys** PU and PR. In general, if (PU,PR) is a valid **key pair** , then (PU+C,PR+C) is not a valid **key pair** for an arbitrary value C. This is because the PU and PR key values meet...will show how this is accomplished. In hybrid cryptographic systems where both a symmetric and **asymmetric algorithm** are implemented, the public and private keys belonging to the **asymmetric algorithm** can be encrypted with keys belonging to the symmetric key algorithm. In that case, the...

...that affect the design choice. For example, the public and private keys belonging to the **asymmetric key algorithm** are typically longer than the keys belonging to the symmetric key algorithm. Also, the possibility ...

...varying lengths must be addressed. 512-bit RSA keys are not uncommon, where a DEA **master key** is generally 128 bits. Thus, the CVE and CVD algorithms must be adjusted to permit...

...vector and the private key can be used to couple the control vector and the **public key** , and the same method of authenticating the key value can be used. Also, handling the...

...private key must be encrypted to ensure that its value does not become

known, the **public key** may also be encrypted to simplify the internal key management design, as then the key...variant key derived from KM, as explained below. If the system master key is an **asymmetric key pair** (PU0,PR0), then PU key record is encrypted with PU0, as explained below. The PU...

...a parameter input to a cryptographic instruction, the PU authenticator is used to validate the **public key** as part of key recovery, before the recovered PU is processed within the cryptographic instruction...

...variant key derived from KM, as explained below. If the system master key is an **asymmetric key pair** (PU0,PR0), then the PR key record is encrypted with PU0, as explained below. The...

...a parameter input to a cryptographic instruction, the PR authenticator is used to validate the **public key** as part of key recovery, before the recovered PR is processed within the cryptographic instruction...

18/5,K/10 (Item 10 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00522867
A hybrid public key algorithm/data encryption algorithm key distribution method based on control vectors
Auf Steuervektoren beruhendes Schlusselverteilungsverfahren mit hybridem Public-Key/DES-Algorithmus
Procede de distribution de cle base sur des vecteurs de commande et utilisant un algorithme hybride a cle publique/DES
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: CH;DE;FR;GB;IT;LI;NL;SE)
INVENTOR:
Matyas, Stephen M., 10298 Cedar Ridge Drive, Manassas, VA 22110, (US)
Johnson, Donald B., 11635 Crystal Creek Lane, Manassa, VA 22111, (US)
Le, An V., 10227 Battlefield Drive, Manassas, Va 22110, (US)
Martin, William C., 1835 Hilliard Lane, Concord, NC 28025, (US)
Prymak, Rostislaw, 15900 Fairway Drive, Dumfries, VA 22026, (US)
Rohland, William S., 4234 Rotunda Road, Charlotte, NC 28226, (US)
Wilkins, John D., P.O. Box 8, Somerville, VA 22739, (US)
LEGAL REPRESENTATIVE:
Schafer, Wolfgang, Dipl.-Ing. (62021), IBM Deutschland Informationssysteme GmbH Patentwesen und Urheberrecht, 70548 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 529261 A2 930303 (Basic)
EP 529261 A3 931118
EP 529261 B1 970212
APPLICATION (CC, No, Date): EP 92111758 920710;
PRIORITY (CC, No, Date): US 748407 910822
DESIGNATED STATES: CH; DE; FR; GB; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: H04L-009/08;
CITED PATENTS (EP A): EP 356065 A; EP 356065 A; EP 356065 A; EP 356065 A; EP 354770 A; EP 354770 A
CITED REFERENCES (EP A):
ICL TECHNICAL JOURNAL vol. 3, no. 2, November 1982, LONDON pages 175 - 188 R. JONES 'Some techniques for handling encipherment keys'
PATENT ABSTRACTS OF JAPAN vol. 015, no. 340 (E-1105)28 August 1991;

ABSTRACT EP 529261 A2

The patent describes a method and apparatus for securely distributing an initial **Data** Encryption **Algorithm** (DEA) key-encrypting key by encrypting a key record (consisting of the key-encrypting key and control information associated with that key-encrypting key) using a **public key algorithm** and a **public key** belonging to the intended recipient of the key record. The patent further describes a method and apparatus for securely recovering the distributed key-encrypting key by the recipient by decrypting the received key record using the same **public key algorithm** and private key associated with the **public key** and re-encrypting the key-encrypting key under a key formed by arithmetically combining the recipient's **master key** with a control vector contained in the control information of the received key record. Thus the type and usage attributes assigned by the originator of the key-encrypting key in the form of a control vector are cryptographically coupled to the key-encrypting key such that the recipient may only use the received key-encrypting key in a manner defined by the key originator.

The patent further describes a method and apparatus to improve the integrity of the key distribution process by applying a digital signature to the key record and by including identifying information (i.e., an originator identifier) in the control information of the key record. The integrity of the distribution process is enhanced by verifying the digital signature and originator identifier at the recipient node. (see image in original document)

ABSTRACT WORD COUNT: 239

LEGAL STATUS (Type, Pub Date, Kind, Text):

Lapse:	030212	B1	Date of lapse of European Patent in a contracting state (Country, date): CH 19970212, LI 19970212, FR 19970711, IT 19970212, NL 19970212, SE 19970512,
Application:	930303	A2	Published application (A1with Search Report ;A2without Search Report)
Change:	930512	A2	Representative (change)
Examination:	930825	A2	Date of filing of request for examination: 930624
Change:	930929	A2	Representative (change)
Search Report:	931118	A3	Separate publication of the European or International search report
Examination:	940309	A2	Date of despatch of first examination report: 940121
Change:	940921	A2	Representative (change)
Grant:	970212	B1	Granted patent
Lapse:	980114	B1	Date of lapse of the European patent in a Contracting State: FR 970711
Lapse:	980121	B1	Date of lapse of the European patent in a Contracting State: CH 970212, LI 970212, FR 970711
Lapse:	980121	B1	Date of lapse of the European patent in a Contracting State: CH 970212, LI 970212, FR 970711
Oppn None:	980204	B1	No opposition filed
Lapse:	980311	B1	Date of lapse of the European patent in a Contracting State: CH 970212, LI 970212, FR 970711, SE 970512
Lapse:	991020	B1	Date of lapse of European Patent in a contracting state (Country, date): CH 19970212, LI 19970212, FR 19970711, IT 19970212, SE 19970512,

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	4295
CLAIMS B	(English)	EPAB97	3572
CLAIMS B	(German)	EPAB97	3301
CLAIMS B	(French)	EPAB97	4231
SPEC A	(English)	EPABF1	13673
SPEC B	(English)	EPAB97	13700
Total word count - document A			17969
Total word count - document B			24804
Total word count - documents A + B			42773

...ABSTRACT A2

The patent describes a method and apparatus for securely distributing an initial **Data** Encryption **Algorithm** (DEA) key-encrypting key by encrypting a key record (consisting of the key-encrypting key and control information associated with that key-encrypting key) using a **public key algorithm** and a **public key** belonging to the intended recipient of the key record. The patent further describes a method...

...key-encrypting key by the recipient by decrypting the received key record using the same **public key algorithm** and private key associated with the **public key** and re-encrypting the key-encrypting key under a key formed by arithmetically combining the recipient's **master key** with a control vector contained in the control information of the received key record. Thus...

18/5,K/11 (Item 11 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

00472875

System for maintaining scrambling security in a communication network

System zur Bewahrung der Verschlusselungssicherheit eines Nachrichtennetzes

Systeme pour le maintien de la securite du codage dans un reseau de communication

PATENT ASSIGNEE:

GENERAL INSTRUMENT CORPORATION OF DELAWARE, (1783080), 181 West Madison Street, Chicago, Illinois 60602, (US), (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;NL;SE)

INVENTOR:

Esserman, James Neil, 3844 Radcliffe Lane, San Diego, California 92122, (US)

Heller, Jerrold A., 4932 Rancho Viejo Drive, Del Mar, California 92014, (US)

LEGAL REPRESENTATIVE:

Hoeger, Stellrecht & Partner (100381), Uhlandstrasse 14 c, 70182 Stuttgart, (DE)

PATENT (CC, No, Kind, Date): EP 485887 A2 920520 (Basic)
EP 485887 A3 921209
EP 485887 B1 970806

APPLICATION (CC, No, Date): EP 91118977 911107;

PRIORITY (CC, No, Date): US 614940 901116

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IT; LI; NL; SE

INTERNATIONAL PATENT CLASS: H04N-007/16;

CITED PATENTS (EP A): EP 127381 A; WO 8806826 A; US 4991208 A; US 5029207 A

CITED REFERENCES (EP A):

IEEE INTERNATIONAL CONFERENCE on CONSUMER ELECTRONICS, 6-8 June, 1990, Rosemont, Illinois, US, pages 316-317; P.J.Y. PERYET: 'Defeating pay-TV pirates with smart cards'

INTERNATIONAL CONFERENCE on SECURE COMMUNICATION SYSTEMS, 22-23 February,

1984, IEE, London , GB, pages 66-69; A.G. MASON: 'A pay-per-view conditional access system for DBS by means of secure over-air credit transmissions';

ABSTRACT EP 485887 A2

A secure communication network serves a plurality of terminals (30, 34, 38) grouped into different security categories. Each terminal includes a replaceable security element (32, 36, 40) containing a security algorithm specific to the security category to which the terminal is assigned. Upon the breach of a particular security version, the security elements in the affected category are replaced with new elements containing a different algorithm. The security elements are relatively low cost, and can be replaced on an as needed or periodic basis to maintain system security. (see image in original document)

ABSTRACT WORD COUNT: 95

LEGAL STATUS (Type, Pub Date, Kind, Text):

Lapse:	20000202	B1	Date of lapse of European Patent in a contracting state (Country, date): GR 19970806, IT 19970806,
Application:	920520	A2	Published application (A1with Search Report ;A2without Search Report)
Search Report:	921209	A3	Separate publication of the European or International search report
Examination:	930428	A2	Date of filing of request for examination: 930227
*Assignee:	940803	A2	Applicant (transfer of rights) (change): GI CORPORATION (1739540) 2200 Byberry Road Hatboro, Pennsylvania 19040 (US) (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;NL;SE)
*Assignee:	940921	A2	Applicant (transfer of rights) (change): GENERAL INSTRUMENT CORPORATION OF DELAWARE (1783080) 181 West Madison Street Chicago, Illinois 60602 (US) (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;NL;SE)
Examination:	950405	A2	Date of despatch of first examination report: 950220
Grant:	970806	B1	Granted patent
Oppn None:	980729	B1	No opposition filed
Lapse:	991020	B1	Date of lapse of European Patent in a contracting state (Country, date): IT 19970806,

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9708W1	1075
CLAIMS B	(German)	9708W1	1060
CLAIMS B	(French)	9708W1	1225
SPEC B	(English)	9708W1	2991
Total word count - document A			0
Total word count - document B			6351
Total word count - documents A + B			6351

...SPECIFICATION from its seeds, which unit key is stored in a secure memory for use in **reproducing** the **common category key** signal when the descrambler is addressed by its unique encrypted category key signal.

As indicated...

18/5,K/12 (Item 12 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00467788
Information processing apparatus with replaceable security element
Informationsverarbeitungsgerat mit auswechselbarem Sicherheitselement
Dispositif de traitement d'information avec element de securite remplacable
PATENT ASSIGNEE:
General Instrument Corporation, (2532981), 101 Tournament Drive, Horsham, PA 19044, (US), (Proprietor designated states: all)
INVENTOR:
Esserman, James Neil, 3844 Radcliffe Lane, San Diego, California 92122, (US)
Moroney, Paul, 1249 Avocet Court, Cardiff, California 92007, (US)
LEGAL REPRESENTATIVE:
Hoeger, Stellrecht & Partner (100381), Uhlandstrasse 14 c, 70182 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 471373 A2 920219 (Basic)
EP 471373 A3 920729
EP 471373 B1 991006
APPLICATION (CC, No, Date): EP 91113757 910816;
PRIORITY (CC, No, Date): US 568990 900817
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: H04N-007/167
CITED PATENTS (EP A): WO 8500491 A; WO 8500491 A; GB 2151886 A; GB 2151886 A; EP 194769 A; EP 132401 A; EP 127381 A
CITED PATENTS (EP B): EP 127381 A; EP 132401 A; EP 194769 A; WO 85/00491 A; GB 2151886 A

ABSTRACT EP 471373 A2
A field upgradeable security system deciphers signals received from a communication network. An information processor (10) includes a receptacle for receiving a replaceable security element (12). The replaceable security element generates a working key (WK) necessary to the operation of the information processor. The working key is communicated to the information processor encrypted under a secret key (A(M)). The information processor decrypts the encrypted working key for use in deciphering a received communication signal. Additional layers of encryption (A(C), U(M), U(C)) can be added to the communications between the information processor and security element to increase the level of security. (see image in original document)
ABSTRACT WORD COUNT: 107
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Oppn None:	000920	B1	No opposition filed: 20000707
Application:	920219	A2	Published application (A1with Search Report ;A2without Search Report)
Lapse:	030212	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19991006, BE 19991006, CH 19991006, LI 19991006, NL 19991006, SE 19991006,
Lapse:	001227	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19991006, BE 19991006, CH 19991006, LI 19991006,
Lapse:	001213	B1	Date of lapse of European Patent in a contracting state (Country, date): BE 19991006, CH 20000111, LI 20000111,

Lapse:	001025	B1	Date of lapse of European Patent in a contracting state (Country, date): BE 19991006,
Lapse:	001220	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19991006, BE 19991006, CH 20000111, LI 20000111,
Lapse:	020605	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19991006, BE 19991006, CH 19991006, LI 19991006, SE 19991006,
Search Report:	920729	A3	Separate publication of the European or International search report
Examination:	921202	A2	Date of filing of request for examination: 921006
*Assignee:	940803	A2	Applicant (transfer of rights) (change): GI CORPORATION (1739540) 2200 Byberry Road Hatboro, Pennsylvania 19040 (US) (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;NL;SE)
*Assignee:	940921	A2	Applicant (transfer of rights) (change): GENERAL INSTRUMENT CORPORATION OF DELAWARE (1783080) 181 West Madison Street Chicago, Illinois 60602 (US) (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;NL;SE)
Examination:	950308	A2	Date of despatch of first examination report: 950120
*Assignee:	981021	A2	Applicant (transfer of rights) (change): NextLevel Systems, Inc. (2532980) 101 Tournament Drive Horsham, PA 19044 (US) (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;NL;SE)
*Assignee:	981021	A2	Previous applicant in case of transfer of rights (change): GENERAL INSTRUMENT CORPORATION OF DELAWARE (1783080) 181 West Madison Street Chicago, Illinois 60602 (US) (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;NL;SE)
*Assignee:	981028	A2	Applicant (transfer of rights) (change): General Instrument Corporation (2532981) 101 Tournament Drive Horsham, PA 19044 (US) (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;NL;SE)
*Assignee:	981028	A2	Previous applicant in case of transfer of rights (change): NextLevel Systems, Inc. (2532980) 101 Tournament Drive Horsham, PA 19044 (US) (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;NL;SE)
Grant:	991006	B1	Granted patent

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9940	1704
CLAIMS B	(German)	9940	1516
CLAIMS B	(French)	9940	1945
SPEC B	(English)	9940	4762
Total word count - document A			0
Total word count - document B			9927
Total word count - documents A + B			9927

...SPECIFICATION signal. Each descrambler has its unique unit key signal

stored in memory for use in **reproducing** the **common category key** signal when the descrambler is addressed by its unique encrypted category key signal. By using...

18/5,K/13 (Item 13 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00396572
Cryptographic method and apparatus for public key exchange with authentication.
Geheimubertragungsverfahren und Einrichtung zum offentlichen Schlusselaustausch mit Authentifizierung.
Procede et dispositif cryptographique d'echange de cle publique avec authentification.
PATENT ASSIGNEE:
TRW INC., (208104), 1900 Richmond Road, Cleveland Ohio 44124, (US), (applicant designated states: DE;FR;GB;IT)
INVENTOR:
Goss, Kenneth C., 1470 Island Court, Oceano California 93445-9464, (US)
LEGAL REPRESENTATIVE:
Allden, Thomas Stanley et al (27631), A.A. THORNTON & CO. Northumberland House 303-306 High Holborn, London WC1V 7LE, (GB)
PATENT (CC, No, Kind, Date): EP 393806 A2 901024 (Basic)
EP 393806 A3 911113
APPLICATION (CC, No, Date): EP 90300115 900105;
PRIORITY (CC, No, Date): US 339555 890417
DESIGNATED STATES: DE; FR; GB; IT
INTERNATIONAL PATENT CLASS: H04L-009/32; H04L-009/08;
CITED PATENTS (EP A): US 4200770 A
CITED REFERENCES (EP A):
IEEE/IEICE GLOBAL TELECOMMUNICATIONS CONFERENCE 1987, CONFERENCE RECORD, Tokyo, 15th - 18th November 1987, vol. 1, pages 108-111, IEEE, New York, US; E. OKAMOTO et al.: "Key distribution system based on identification information";

ABSTRACT EP 393806 A2
A technique for use in a **public key** exchange cryptographic system, in which two user devices establish a **common session key** by exchanging information over an insecure communication channel, and in which each user can authenticate the identity of the other, without the need for a key distribution center. Each device has a previously stored unique random number Xi, and a previously stored composite quantity that is formed by transforming Xi to Yi using a transformation of which the inverse in computationally infeasible; then concatenating Yi with a publicly known device identifier, and digitally signing the quantity. Before a communication session is established, two user devices exchange their signed composite quantities, transform them to unsigned form, and authenticate the identity of the other user. Then each device generates the same **session key** by transforming the received Y value with its own X value. For further security, each device also generates another random number X(min)i, which is transformed to a corresponding number Y(min)i. These Y(min)i values are also exchanged, and the **session key** is generated in each device, using a transformation that involves the device's own Xi and X(min)i numbers and the Yi and Y(min)i numbers received from the other device.
ABSTRACT WORD COUNT: 204

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	901024 A2	Published application (A1with Search Report ;A2without Search Report)
Search Report:	911113 A3	Separate publication of the European or International search report
Examination:	920701 A2	Date of filing of request for examination: 920501
Examination:	940406 A2	Date of despatch of first examination report: 940216
Refusal:	941228 A2	Date on which the European patent application was refused: 940812

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	1356
SPEC A	(English)	EPABF1	5968
Total word count - document A			7324
Total word count - document B			0
Total word count - documents A + B			7324

...ABSTRACT A2
A technique for use in a **public key** exchange cryptographic system, in which two user devices establish a **common session key** by exchanging information over an insecure communication channel, and in which each user can authenticate...

...form, and authenticate the identity of the other user. Then each device generates the same **session key** by transforming the received Y value with its own X value. For further security, each...

...corresponding number Y(min)i. These Y(min)i values are also exchanged, and the **session key** is generated in each device, using a transformation that involves the device's own Xi...

18/5,K/14 (Item 14 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00141732
Key signal encryption and distribution system for controlling scrambling and selective, remote descrambling of television signals.
System zur Verschlusselung und Verteilung eines Schlusselsignals zur gesteuerten Verschlusselung und selektiven empfangerseitigen Entschlusselung von Fernsehsig
Systeme de cryptage et de distribution d'un signal de cryptage pour cryptage commande et decryptage selectif a distance de signaux de television.
PATENT ASSIGNEE:
M/A-COM GOVERNMENT SYSTEMS, INC., (773980), 3033 Science Park Road, San Diego California 92121, (US), (applicant designated states: BE;DE;FR;GB;IT;NL;SE)
CABLE/HOME COMMUNICATION CORP.,, (890530), 6262 Lusk Boulevard, San Diego California 92121, (US), (applicant designated states: BE;DE;FR;GB;IT;NL;SE)
INVENTOR:
Gilhousen, Klein S., 4039 Calgary Avenue, San Diego California 92122, (US)
Newby, Charles F., Jr., 1530 Norran Street, El Cajon California 92021, (US)
Karl E. Moerder, 13360 Whitewater Drive, Poway California 92064, (US)

LEGAL REPRESENTATIVE:
Blatchford, William Michael et al , Withers & Rogers 4 Dyer's Buildings Holborn, London EC1N 2JT, (GB)
PATENT (CC, No, Kind, Date): EP 127381 A1 841205 (Basic)
EP 127381 B1 880406
APPLICATION (CC, No, Date): EP 84303320 840516;
PRIORITY (CC, No, Date): US 498800 830527
DESIGNATED STATES: BE; DE; FR; GB; IT; NL; SE
INTERNATIONAL PATENT CLASS: H04N-007/16;

ABSTRACT EP 127381 A1
Key signal encryption and distribution system for controlling scrambling and selective, remote descrambling of television signals.
A system and method for scrambling and selectively descrambling television signals tnat are transmined to subscribers' descramblers in a subscription television system. A working key signal is generated by processing an "initialization vector" signal in accordance with the DES algorithm upon the algorithm being keyed by either a common category key signal or a signal having a predetermined relationship to the common category key signal. A unique encryption keystream is generated by processing the initialization vector signal in accordance with the DES algorithm upon the algorithm being keyed by the working key signal. A television signal is scrambled in accordance with the unique encryption keystream to provide a scrambled television signal. A plurality of unique encrypted category key signals individually addressed to different selected subscribers' descramblers are generated by processing the initial common category key signal in accordance with the DES algorithm upon the algorithm being keyed by a plurality of different "unit key" signals unique to different selected descramblers. The scrambled television signal, the initidiization vector signal, and the plurality of encrynted category key signals are broadcast to the descramblers. A corresponding tier of DES algorithms are employed at the descrambler to reproduce the encryption keystream; and the TV signal is descrambled in accordance therewith. Each descrambler has its unique unit key signal stored in a secure memory for use in **reproducing** the **common category key** signal when the descrambler is addressed by its unique encrypted category key signal.
ABSTRACT WORD COUNT: 258

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	841205	A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	850807	A1	Date of filing of request for examination: 850529
Change:	860709	A1	Inventor (change)
Examination:	860716	A1	Date of despatch of first examination report: 860603
*Assignee:	871021	A1	Applicant (transfer of rights) (change): M/A-COM GOVERNMENT SYSTEMS, INC. (773980) 3033 Science Park Road San Diego California 92121 (US) (applicant designated states: BE;DE;FR;GB;IT;NL;SE), CABLE/HOME COMMUNICATION CORP., (890530) 6262 Lusk Boulevard San Diego California 92121 (US) (applicant designated states: BE;DE;FR;GB;IT;NL;SE)
Grant:	880406	B1	Granted patent
Oppn None:	890329	B1	No opposition filed

LANGUAGE (Publication,Procedural,Application): English; English; English

...ABSTRACT descrambler has its unique unit key signal stored in a secure memory for use in **reproducing** the **common category key** signal when

the descrambler is addressed by its unique encrypted category key signal.

18/5,K/15 (Item 15 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01009621
SOFTWARE AND SYSTEMS FOR FACILITATING E-BUSINESS
LOGICIEL ET SYSTEMES DE COMMERCE ELECTRONIQUE
Patent Applicant/Assignee:
LINKWARE SYSTEMS B V, Kampweg 27, NL-3981 EX Bunnik, NL, NL (Residence), NL (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
KLYHN Henning, Kampweg 27, NL-3981 EX Bunnik, NL, NL (Residence), NL (Nationality), (Designated only for: US)
Legal Representative:
de HOOP Eric (agent), Octrooibureau Vriesendorp & Gaade, P.O. Box 266, NL-2501 AW The Hague, NL,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200338714 A2 20030508 (WO 0338714)
Application: WO 2002NL702 20021104 (PCT/WO NL0200702)
Priority Application: US 2001335298 20011102
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-017/60
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 20442

English Abstract
The invention pertains to a method for managing and executing business transactions in a product/service chain, wherein at least one closed user group is defined by installing, in memory means on first remote computer means, a list of trusted business partners forming said product/service chain, each business partner maintaining, on further remote computer means, at least one software system and at least one database for managing internal business processes, like resource management, contract/proposal management, logistics management, financial management, etcetera, wherein said transactions are managed and executed by management software obtaining data from several databases of several business partners.

French Abstract
L'invention concerne un procede de gestion et de mise en oeuvre d'operations commerciales dans une filiere de production/service. Ce procede consiste a former au moins un groupe ferme d'usagers a partir d'une liste de partenaires commerciaux de confiance formant ladite filiere de production/service et a enregistrer ce groupe dans la memoire d'un premier dispositif informatique a distance. Chaque partenaire commercial utilise au moins un systeme logiciel et au moins une base de donnees mis en oeuvre sur d'autres dispositifs informatiques a distance,

destines a la gestion des procedes administratifs internes, tels que la gestion des ressources, la gestion des marches/propositions, la gestion logistique, la gestion financiere, etc. Les operations sont gerees par un logiciel de gestion alimente par les bases de donnees des partenaires commerciaux.

Legal Status (Type, Date, Text)
Publication 20030508 A2 Without international search report and to be republished upon receipt of that report.

Fulltext Availability:
Claims

Claim
... according to claim 14 or 15, wherein the metascript comprises a security code comprising a **master key** , a **public key** , a **session key** and an access tag; wherein a remote computer randomly refreshes the **public key** .

17 Method for managing and- executing a chain of business transactions in a product/service...comprising encrypted links to data on
remote computers, wherein the links are encrypted using a **master key** , a **public key** ,, a **session key** and a configuration access tag,

23 Datastructure according, to claim 22, wherein the public key...

(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: B41J-002/07
International Patent Class: B41J-002/17; G06F-003/12
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 140412

English Abstract
An image printing apparatus includes a print head for printing images. A microcontroller that includes a wafer substrate is provided. Processor circuitry is positioned on the wafer substrate. Print head interface circuitry is also positioned on the wafer substrate and is connected between the processor circuitry and the print head. The print head interface circuitry is configured to facilitate communication between the processor circuitry and the print head. Bus interface circuitry that is discrete from the print head interface circuitry is connected to the processor circuitry so that the processor circuitry can communicate with devices other than the print head via a bus.

French Abstract
L'invention concerne un appareil d'impression d'images comprenant une tete d'impression permettant d'imprimer des images, ainsi qu'une micro-unite de commande comprenant un substrat de plaquette. Un ensemble de circuits de processeur est positionne sur le substrat de plaquette. Un ensemble de circuits d'interface de la tete d'impression est egalement positionne sur le substrat de plaquette et est connecte entre l'ensemble de circuits du processeur et la tete d'impression. L'ensemble de circuits d'interface de la tete d'impression est concu pour faciliter la communication entre l'ensemble de circuits du processeur et la tete d'impression. Un ensemble de circuits d'interface bus, qui est distinct de celui de la tete d'impression, est connecte a l'ensemble de circuits du processeur, de maniere que celui-ci puisse communiquer avec d'autres dispositifs que la tete d'impression, via un bus.

Legal Status (Type, Date, Text)
Publication 20030220 A1 With international search report.
Examination 20030417 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... VLIW Input FEFO 78 is the Image Sensor Interface (ISI 83). The ISI 83 takes **data** from the Image Sensor and writes it to the FIFO. A VLIW process takes it...and then combined with the other PU e.g 178 status bits to update the **Common** Status Register 200. The microcode for determining the output status bit takes the following form...205, for multiple types of interpolations and multiply/accumulates
Barrel Shift block 206, for shifting **data** as required
In block 207, for accepting data from the external crossbar switch 183
Out...

18/5,K/23 (Item 23 from file: 349)

00876811 **Image available**

SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR DEVICE, OPERATING SYSTEM, AND NETWORK TRANSPORT NEUTRAL SECURE INTERACTIVE MULTI-MEDIA MESSAGING

SYSTEME, PROCEDE ET PRODUIT PROGRAMME D'ORDINATEUR POUR APPAREIL, SYSTEME D'EXPLOITATION ET MESSAGERIE MULTIMEDIA INTERACTIVE RESEAU, NEUTRE ET SECURISEE

Patent Applicant/Assignee:
STORYMAIL INC, 15729 Los Gatos Boulevard, Los Gatos, CA 95032, US, US (Residence), US (Nationality)
Inventor(s):
ILLOWSKY Daniel H, 21363 Dexter, Cuptertino, CA 95014, US,
WENOCUR Michael L, 4057 Amaranta Avenue, Palo Alto, CA 94306, US,
BALDWIN Robert W, 990 Amarillo Avenue, Palo Alto, CA 94303, US,
SAXBY David B, 14946 Granite Court, Saratoga, CA 95070, US,
Legal Representative:
ANANIAN R Michael (et al) (agent), Flehr Hohbach Test Albritton & Herbert LLP, 4 Embarcadero Center, Suite 3400, San Francisco, CA 94111-4187, US
,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200210962 A1 20020207 (WO 0210962)
Application: WO 2001US23713 20010727 (PCT/WO US0123713)
Priority Application: US 2000627357 20000728; US 2000627358 20000728; US 2000627645 20000728; US 2000628205 20000728; US 2000706606 20001104; US 2000706609 20001104; US 2000706610 20001104; US 2000706611 20001104; US 2000706612 20001104; US 2000706613 20001104; US 2000706614 20001104; US 2000706615 20001104; US 2000706616 20001104; US 2000706617 20001104; US 2000706621 20001104; US 2000706661 20001104; US 2000706664 20001104; US 2001271455 20010225; US 2001912715 20010725; US 2001912936 20010725; US 2001912905 20010725; US 2001912773 20010725; US 2001912885 20010725; US 2001912860 20010725; US 2001912941 20010725; US 2001912901 20010725; US 2001912772 20010725
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-017/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 169299

English Abstract
System, method, signal, operating model, and computer program for electronic messaging. Systems and method for providing security for communication of electronic messages, interactive sessions, software downloads, software upgrades, and other content from a source to a receiving device as well as signals used for such communications (304, 309, 308, 324, 342, 338, 334, 330, 326). Systems, methods, signals, device architectures, data formats, and computer program structures for providing authentication, integrity, confidentiality, non-repudiation, replay protection, and other security properties while minimizing the network (306) bandwidth, computational resources and manual user

interactions (314) required to install, enable, deploy and utilize these security properties. System, device, method, computer program, and computer program product for searching and slecting data and control elements in message procedural/data sets for automatic and complete portrayal of message to maintain message intent.

French Abstract

Systeme, procede, signal, modele operatoire et programme d'ordinateur pour messagerie electronique. Systemes et procede permettant de securiser la communication de donnees de messages electroniques, sessions interactives, telechargements de logiciels, mises a jour de logiciels et autres contenus d'une source a un appareil recepteur ; signaux utilises pour ce type de communication (304, 309, 308, 324, 342, 338, 334, 330, 326). Systemes, procedes, signaux, architectures d'appareils, formats de donnees et structures de programmes d'ordinateur assurant l'authentification, l'integrite, la confidentialite, la non-repudiation, la protection contre la reinsertion ainsi que d'autres proprietes de securite tout en reduisant la bande passante du reseau (306), ressources informatiques et interactions manuelles de l'utilisateur (314) requises pour l'installation, l'activation, le deploiement et l'utilisation de ces proprietes de securite. Systeme, appareil, procede, programme d'ordinateur et produit programme d'ordinateur permettant de rechercher et de selectionner des elements de donnee et de commande dans des procedures relatives aux messages et des ensembles de donnees pour obtenir une representation automatique et complete du message et preserver l'intention du message.

Legal Status (Type, Date, Text)

Publication	20020207	A1 With international search report.
Publication	20020207	A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination	20030116	Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:

Claims

Claim

... using Signed-Inside-Enveloped-Data to provide the software signing, and using a fixed Recipient **public key** to which all receiving software knows the private key for the encryption, rather than providing ...

...89, wherein the Signed-inside-Enveloped-Data primitive provides a component for setting up a **session key** with a new entity for which the Sender knows the Recipient's **public key** . 117.Themethodinclaiml16, whereintheSenderknowstherecipienrspublickeybyanyoneof: (i)a plain text request of the certificate of the Recipient, (ii...

...primitive with the appropriate keys. 123. The method in claim 89, wherein authentication for a **session key** is provided by using the Encrypted-Data primitive with values that are produced by the...Secure Response message protocol is implemented using the Signed-Inside-Enveloped-Data primitive with a **public key** of the Recipient that is included inside the message to which this is a response ...

...133, wherein the message includes a Certificate and the Signed-InsideEnveloped-Data primitive with a **public key** of the Recipient is inside the Certificate that is verified by the Sender of the

key and destination address and Client's public and private key and certificate chain from one...

...the Entity in order to respond to a message from the Entity, the Entity's **public key** and matching destination address of the Entity from a
trusted storage means;
B. extracting, by...

...the Entity in order to respond to a message from the Entity, the Entity's **public key** and matching destination address of the Entity from a
trusted storage means;
B. extracting, by ...for the received response message. 254. The method in Claim 252, wherein the Entity's **public key** comprises an RSA or RSA-based key. 255. The method in Claim 252, wherein the...

...destination address comprises an e-mail address. 256. The method in Claim 252, wherein the **public key** and matching destination address have been verified previously using a digital signature (verified with a trusted **public key**) or cryptographic checksurn (verified with a trusted key derived from a **Master Key** or **Session Key** or Message Key). 257. The method in Claim 252, wherein the trusted source or storage ...

...the method comprising the steps of. extracting, by the Client, information including the Entity's **public key** and matching destination address and the Client's public and private key and certificate chain...

...Compact Certificate as explained earlier, or chain of Compact Certificates leading to a trusted root **public key** . 270. The method of claim 252, wherein the trusted source or storage means comprises a Compact Certificate as explained earlier, or chain of Compact Certificates leading to a trusted root **public key** . 271. A hardware architecture neutral executable program structure for execution in a processor,
said program...

18/5,K/24 (Item 24 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00864440 **Image available**
METHOD AND APPARATUS FOR ENHANCING NETWORK SECURITY PROTECTION SERVER PERFORMANCE
PROCEDE ET APPAREIL DESTINES A AMELIORER LES PERFORMANCES DU SERVEUR DE PROTECTION DE SECURITE DE RESEAU
Patent Applicant/Assignee:
INGRIAN SYSTEMS INC, 3071 Edison Way, Redwood City, CA 94063, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
SHACHAM Hovav, 3826 Mumford Place, Palo Alto, CA 94306, US, US (Residence), US (Nationality), (Designated only for: US)
BONEH Dan, 3349 Louis Road, Palo Alto, CA 94303, US, US (Residence), IL (Nationality), (Designated only for: US)
BERI Sanjay, 562 Kendall Avenue, Unit #4, Palo Alto, CA 94306, US, US (Residence), CA (Nationality), (Designated only for: US)
Legal Representative:

GREGORY Richard L Jr (agent), Wilson Sonsini Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94304-1050, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200197443 A2-A3 20011220 (WO 0197443)
Application: WO 2001US18878 20010612 (PCT/WO US0118878)
Priority Application: US 2000211023 20000612; US 2000211031 20000612
Parent Application/Grant:
Related by Continuation to: US 2000211023 20000612 (CIP); US 2000211031 20000612 (CIP); US Not furnished (CIP)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-009/30
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12621

English Abstract
Presented is a method and system for improving the efficiency of network security protections communication protocols such as Secure Socket Layer ("SSL") using enhanced Rivest-Shamir-Adleman ("RSA") encryption and decryption techniques. During the establishment of the initial handshake of SSL communications, where a client is coupled to a server, the server generates a RSA public/private key pair. The public key is formed using two distinct prime numbers. By reducing the size of these prime numbers and arriving at the decrypted message using the Chinese Remainder Theorem, the efficiency of establishing a secure communications session is increased. Likewise if during generation of the public key, the prime numbers possess a mathematical relationship to the public key such that the prime numbers on the order of a third of the size of the public key then the efficiency of establishing the initial handshake is again improved.

French Abstract
L'invention concerne un procede et un systeme destines a ameliorer l'efficacite du protocole de communication des protections de securite de reseau, tel que le protocole SSL, au moyen de techniques de chiffrement et de dechiffrement RSA. Pendant l'etablissement d'une liaison initiale de communication SSL, dans laquelle un client est relie a un serveur, le serveur genere une paire de cles RSA publique/privee. La cle publique est constituee de deux nombres premiers distincts. En reduisant la taille de ces nombres premiers et en obtenant le message dechiffre au moyen du theoreme chinois du reste, l'efficacite d'etablissement d'une session de communication securisee est augmentee. De meme, si pendant la generation de la cle publique, les nombres premiers possedent une relation mathematique avec la cle publique telle que les nombres premiers sont de l'ordre d'un troisieme de la taille de la cle publique, alors l'efficacite d'etablissement de la liaison initiale est a nouveau amelioree.

Legal Status (Type, Date, Text)
Publication 20011220 A2 Without international search report and to be republished upon receipt of that report.

Search Rpt 20030508 Late publication of international search report
Republication 20030508 A3 With international search report.

Fulltext Availability:
Claims

Claim
... are combined using the
Chinese Remainder Theorem, wherein computational efficiency is improved;
and
establishing a **common session key** between the web server and the
client using R.)i

10 The method of claim...combined using the Chinese
5 Remainder Theorem, wherein computational efficieney is improved and
establish a **common session key** between the web server and the
client
using R.

30 An electromagnetic medium, comprising executable...

...are combined using the Chinese
Rernainder Theorem, wherein. computational efficiency is improved; and
establish a **common session key** between the web server and the
client
using R.
0

31 A computer-readable medium...

facility for ensuring...

18/5,K/26 (Item 26 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00762353 **Image available**
WEB ENVIRONMENT ACCESS CONTROL
CONTROLE D'ACCES DANS UN ENVIRONNEMENT WEB
Patent Applicant/Assignee:
QINETIQ LIMITED, 85 Buckingham Gate, London SW1 6TD, GB, GB (Residence), GB (Nationality), (For all designated states except: US)
HEARN Tina (heiress of the deceased inventor), 8 Redwing Close, Halfkey, Malvern WR14 1UN, GB, GB (Residence), GB (Nationality), (Designated only for: US)
Inventor(s):
HEARN David Brian (deceased),
Patent Applicant/Inventor:
WILKINSON Timothy John, DERA Malvern, St. Andrews Road, Malvern, Worcs WR14 3PS, GB, GB (Residence), GB (Nationality), (Designated only for: US)
Legal Representative:
BOWDERY A O (agent), Qinetiq Limited, IP Formalities, A4 Bldg., Cody Technology Park, Ively Road, Farnborough, Hampshire GU14 0LX, GB,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200075754 A2-A3 20001214 (WO 0075754)
Application: WO 2000GB2049 20000606 (PCT/WO GB0002049)
Priority Application: GB 9913165 19990608
Designated States: CA GB US
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6056

English Abstract
An access control system and method in a web environment having pre-encrypted files on a web server decryption keys provided to authorised users and a trusted user proxy for controlling file access and decrypting files received, in which files are encrypted using a file key (FK), and the FK is encrypted using a Group Encryption Key (GEK), and the user proxy has a Group Decryption Key (GDK) to decrypt the FK and the file. Each encrypted file is labelled with an Access Control Expression (ACE) which indicates which users or groups of users are authorised to decrypt and observe the file; this provides a secure client server system having pre-encrypted documents on the web-server, released to a decryption proxy on the client side, which controls access to, and decrypts the documents the client is allowed to see.

French Abstract
L'invention concerne un dispositif et un procede de controle d'acces dans un environnement web contenant des fichiers precryptes sur un serveur web, des cles de cryptage fournies aux utilisateurs autorises et un utilisateur de confiance mandate pour controler l'acces aux fichiers et decrypter les fichiers recus. Les fichiers sont cryptes au moyen d'une cle de fichier, FK, laquelle est chiffree au moyen d'une cle de cryptage de groupe, GEK. L'utilisateur mandate possede une cle de decryptage de

groupe, GDK, pour dechiffrer la FK et le fichier. Une etiquette d'expression de controle d'acces (ACE) est apposee sur chaque fichier crypte indiquant les utilisateurs ou groupes d'utilisateurs habilites a decrypter et a consulter le fichier, ce qui permet de disposer d'un systeme client-serveur securise dont les documents precryptes sur le serveur web sont liberes a l'attention d'un mandataire de decryptage du cote client, qui controle l'acces aux documents et qui les decrypte a l'attention du client habilite a les consulter.

Legal Status (Type, Date, Text)

Publication	20001214	A2 Without international search report and to be republished upon receipt of that report.
Examination	20010222	Request for preliminary examination prior to end of 19th month from priority date
Search Rpt	20020606	Late publication of international search report
Republication	20020606	A3 With international search report.

Fulltext Availability:
Claims

Claim
... files by means of a File Key (FK), encrypting the FK by means of a **Group** Encryption **Key** , and providing only the limited number of groups with a means of decrypting the FK...

...header containing information including
the ACE
enabling authorised users to decrypt the encrypted file;
a **group** encryption **key** (GEK) is generated for defined groups of authorised
users;
a GEK encrypts the FK and...
...Group ID, the FK in GEK, and the ACE;
delivering to the users proxy a **group** decryption **key** (GDK)
user retrieves file and proxy examines incoming encrypted file ACE in the header to see how or if decryption can take place;
users **group** decryption **key** (GDK) is used to decrypt the file key (FK) from the
header;
the file is...

...must be considered untrustworthy, could gain access to all data subsequently released by replacing the **group** encryption **key** with one for which it knows the corresponding **group** decryption **key** .
Preferably the system uses asymmetric keys. The advantage of asymmetric cryptography is that it gives...and this is used to encrypt the file.
This key is called the file's **data key** . The resulting encrypted data is prepended with a header before being'released to the web...

...The header contains the information that allows legitimate recipients to decrypt the encrypted data. An **asymmetric key pair** is generated for each group in the access control scheme. This **key pair** is used to distribute a file's **data key** to those who are permitted to observe the file. One key of the pair is...
...In the simple case where the ACE is just a single group, the file's **data key** is encrypted using the group's encryption key. The result is placed in the header...

...with the file's label, as shown in figure 1. The way in which the **data key** is encrypted in general is explained below. A file's header

contains the file's ACE, the file's **data key** encrypted in a way determined by the file's ACE, and the file's data. The ftinction for encrypting the **data key** of a file D whose ACE is A is denoted H(D,A), and is...

...H(D, (x1y) & z) = H(D, (x & z) (y & z))
where
D is the file **data key**
G is a simple ACE of one group
x, y and z are arbitrary ACEs...

...key associated with
group G
To observe a file, it must be decrypted using its **data key** . This can be
recovered from the file's header if certain group decrypting keys are known. The ACE determine's which combinations of group decrypting keys permit the **data key** to be recovered. The ftniction that is used to recover a **data key** from the encrypted data E and ACE A in the header is denoted R(E...

...observe a file, the ACE in the header is examined to determine how the encrypted **data key** should be recovered. In the simple case, where the label is just a single group, the group's decryption key is used to recover the file's **data key** from the header. Once the **data key** is obtained, the file's data can be decrypted. If the group's decryption key ...

...the browser knows how to handle the data in the normal way. Most applications of **public key** cryptography assume that a user's application software can be trusted ...give the recipient access to all files released to the group. Similarly, a file's **data key** is protected, otherwise this would give the recipient access to the particular file. However, once...

...of controlling the release of data while using untrustworthy application software. Protecting a file's **data key** from disclosure also affords extra protection to the **group** decryption **key** . A user in possession of a document key, and the same key encrypted with a **group** encryption **key** , has the potential to mount a brute force attack to obtain the **group** decryption **key** . With a single document key, the user has only a small amount of information on...

...must be considered untrustworthy, could gain access to all data subsequently released by replacing the **group** encryption **key** with one for which it knows the corresponding **group** decryption **key** . Note that, having protected both the encrypting and decrypting keys from disclosure and modification, it...

...key can be changed easily. It is simply a matter of recovering the original file **data key** , using the decrypting key of some group which can access it, decrypting the data, and...

...user's workstation. One way of 1 5 achieving this is to make use of **public key** technology. Each proxy would be identifiable by a distinguished name and associated **public key** , most likely wrapped together into an identity certificate. The proxy would hold the complementary private key in private local storage. An administrator wishing to place a consumer **group** decryption **key** into a proxy would obtain the identity certificate corresponding to the proxy. After

verifying the certificate, the **public** . **key** contained within it can be used to encrypt a **group** **key** for forwarding to the proxy. Only a holder of the proxies' private key can unwrap the **group** **key** . At this point the message containing the hidden **group** **key** can be presented to the user of the system by, for example, electronic messaging. Once...

...has been inserted into the proxy, the proxy can unwrap the message to reveal the **group** **key** and place it in private storage. Additional fields could be associated with the key, such...

...the proxy could generate its own private key at installation time, and export the corresponding **public** **key** for signature by a certification authority. While the ultimate solution is to distribute keys through a **public** **key** infrastructure, as discussed above, a lighter-weight alternative is possible using the security mechanisms of...

18/5,K/27 **(Item 27 from file: 349)**

00745762 **Image available**
MULTI-NODE ENCRYPTION AND KEY DELIVERY
CHIFFREMENT MULTINOEUD ET REMISE DE CLES
Patent Applicant/Assignee:
KONINKLIJKE PHILIPS ELECTRONICS N V, Groenewoudseweg 1, NL-5621 BA Eindhoven, NL, NL (Residence), NL (Nationality)
Inventor(s):
ROSNER Martin, Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL
EPSTEIN Michael A, Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL
PASIEKA Michael, Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL
Legal Representative:
FAESSEN Louis M H, Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL
Patent and Priority Information (Country, Number, Date):
Patent: WO 200059154 A1 20001005 (WO 0059154)
Application: WO 2000EP1895 20000306 (PCT/WO EP0001895)
Priority Application: US 99126168 19990325; US 99434156 19991104
Designated States: CN JP KR
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04L-009/08
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6441

English Abstract
The common encryption of content material is provided for decryption at a plurality of destination devices, each destination device having a unique private key of a public-private key pair. A multiple device key exchange is utilized to create a session key for encrypting the content material that is based on each of the public keys of the plurality of destination devices. The content material is encrypted using this session key. A partial key is also created for each of the intended destination devices that relies upon the private key of the destination device to form a decryption key that is suitable for decrypting the encrypted content material. The encrypted content material and the corresponding partial key are communicated to each destination device via potentially insecure

means, including broadcast over a public network. Each destination device decrypts the encrypted content material using the decryption key that is formed from its private key and the received partial key. Including or excluding the public key of selected destination devices in the creation of the session key effects selective encryption.

French Abstract
L'invention concerne le chiffrement ordinaire d'un contenu destine au decryptage au niveau de plusieurs dispositifs destinataires, chaque dispositif possedant une cle privee unique d'une paire de cles privees-publiques. On utilise un echange de cles du dispositif multiple pour creer une cle de session permettant de chiffrer le contenu qui est fonde sur chacune des cles publiques de plusieurs dispositifs destinataires. Le contenu est chiffre a l'aide de cette cle de session. On cree egalement une cle partielle pour chacun des dispositifs destinataires souhaites qui depende de la cle privee du dispositif destinataire pour constituer une cle de decryptage appropriee au decryptage du contenu chiffre. Ce dernier et la cle partielle correspondante sont communiques a chaque dispositif destinataire par le biais d'un dispositif potentiellement non protege, y compris la diffusion sur un reseau publique. Chaque dispositif destinataire decrypte le contenu code a l'aide de la cle de decryptage qui est constituee a partir de sa cle privee et de la cle partielle recue. Inclure ou exclure la cle publique des dispositifs destinataires selectionnes lors de la creation de la cle de session agit sur le chiffrement selectif.
Legal Status (Type, Date, Text)
Publication 20001005 A1 With international search report.

Fulltext Availability:
Claims

Claim
... key (25 la-281a) of a
public-private key pair, the method comprising:
creating a **session key** (22 1) based on a combination of each public key (25 1 a
281 a...

...each partial key being configured to provide a decryption key (255-285) corresponding to the **session key** (221) when combined with the private key (25 I bI 0 281b) of each corresponding destination device and a **public group key** (212a), encrypting the content material (20 1) based on the **session key** (22 1) to create
encrypted content material (23 1), and
communicating the encrypted content material...

...a) of the plurality of destination devices (250-280),
the plurality of keys including:
a **session key** (221) for encrypting the content material (201), and
a plurality of partial keys (225-228...

...each partial key being configured to provide a decryption key (255-285) corresponding to the **session key** (22 1) when combined with the private key (25 lb2 8 lb) of each corresponding destination device and a **public group key** (212a), and an encrypter (230) that is configured to encrypt the content material (201) based on the **session key** (22 1) to create encrypted content material (23 1).
. The source device (21 0) of...

...one destination device (250).

10 The source device (21 0) of claim 9, wherein
the **session key** (221) is further based on a source device private key (212b)
corresponding to the **public group key** (212a), and
the transmitter (240) is further configured to communicate the **public group key** (212a) to the at least one destination device (250).

11 The source device (21 0...a second key (225),
the encrypted content material (23 1) being encrypted based on a **session key**
(22 1) that is based on a plurality of public keys (25 1 a-28 I a),
the first key (212a) corresponding to a **public group key** (212a), and
the second key (225) being based on a subset (26 1 a-28...

...first key (212a), the second key (225), and a private key (25 lb) of a **public** -private **key pair** whose corresponding **public key** (25 1 a) is included in the plurality of public keys (25 1 a28 1...

18/5,K/28 (Item 28 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00518261 **Image available**
CRYPTOGRAPHIC KEY-RECOVERY MECHANISM
MECANISME D'EXTRACTION DE CLE CRYPTOGRAPHIQUE
Patent Applicant/Assignee:
FORTRESS TECHNOLOGIES INC,
FRIEDMAN Aharon,
BOZOKI Eva,
Inventor(s):
FRIEDMAN Aharon,
BOZOKI Eva,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9949613 A1 19990930
Application: WO 99US3665 19990219 (PCT/WO US9903665)
Priority Application: US 9875330 19980220
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: H04L-009/08
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4615

English Abstract
Nodes I, I=1, N are communicating with each other encrypted. They each have static private (Si) and public (Pi) keys, which never change and dynamic private (Sidyn) and public (Pidyn) keys, which are functions of time (t). A key recovery authority (KRA) also has static private (SKRA) and public (PKRA) keys, which never change. The KRA exchanges static public keys with each of the nodes, thus develops a static common key (session key), KKRA,i, with each of them using, for example, the Diffie-Hellman protocol. The KRA maintains a list of the static public

keys of all nodes. Thus, the (static) session key with any of the nodes can be "recovered" at any time. When two nodes, say i and j, exchange their dynamic public keys (encrypted with their static session key Kstij(t)), then each one attaches its dynamic secret key, encrypted with the static session key between it and the KRA. A time stamp is also included. With knowledge of the session key, KKRA,i, which can be recovered from the KRA, the dynamic private keys of each node, Sidyn(t), can be recovered (and Pidyn(t) calculated) from a recording of any session (70). From Sidyn(t) and Pjdyn(t) one can calculate the dynamic session key between the two nodes (Ki,jdyn(t)) (75). However, all other parties are still protected since their dynamic public keys are exchanged encrypted. Note that all nodes are still protected, and their session concealed, because their private keys are encrypted.

French Abstract
Les noeuds I, I=1, N communiquent entre eux de maniere cryptee. Chacun possede des cles privee (Si) et publique (Pi) statiques, qui ne changent jamais, et des cles privee (Sidyn) et publique (Pidyn) dynamiques, qui sont fonction du temps (t). Une autorite d'extraction de cle (KRA) possede egalement des cles privee (SKRA) et publique (PKRA) statiques, qui ne changent jamais. L'autorite d'extraction de cle echange les cles publiques statiques avec chacun des noeuds, ce qui developpe une cle commune statique (cle de session) (KKRA,i), chaque noeud utilisant, par exemple, un protocole de Diffie-Hellman. L'autorite d'extraction conserve une liste des cles publiques statiques de tous les noeuds. La cle de session (statique) avec n'importe quel noeud peut donc etre "extraite" a tout moment. Quand deux noeuds, I et j par exemple, echangent leurs cles publiques dynamiques (cryptees avec leur cle de session statique (Kstij(t)), chacun attache sa cle secrete dynamique, cryptee avec la cle de session statique entre lui et l'autorite d'extraction. Une indication de date et d'heure est ajoutee. En connaissant la cle de session (KKRA,i), qui peut etre extraite a partir de l'autorite d'extraction, il est possible d'extraire les cles privees dynamiques de chaque noeud (Sidyn(t)) (et de calculer Pidyn(t)) a partir d'un enregistrement de n'importe quelle session (70). On peut aussi calculer la cle de session dynamique entre les deux noeuds (Ki,jdyn(t)) a partir de Sidyn(t) et de Pjdyn(t) (75). Cependant, toutes les autres parties sont encore protegees puisque leurs cles publiques dynamiques sont echangees de maniere cryptee; en particulier, tous les noeuds sont proteges et leurs sessions cachees, puisque leurs cles privees sont cryptees.

Fulltext Availability:
Claims

Claim
... public key of each of said first and second nodes stored therein; determining a static **common session key** , 'C'KRAA, between said KRA and said first
1 0 nodes, based on said P...

...node, (SBd"(T)), based on said
EKW%R,1f,B) (SBI(T));
determining a dynamic **public key** of said second node, PBdy'(T), based on said
2 0 SBdy'(T); and
determining said dynamic **common key** , Kd",@,B(T), based on said SAdI'(T) and said PB'@'% for decrypting messages transmitted...

...retrieving a dynamic private key, Sady') from said first node which is encrypted with a **common session key** between said first node and a key recovery authority (KRA) third

party node KKRAA;
wherein said Sad" encrypted with said KKR&A is utilized for decrypting said dynamic **public key** of said first node.

5 The method of claim 4, wherein said step of determining...

...and
a dynamic private key, Sady') from said first node which is encrypted with a **common session key** between said first node and a key recovery authority (KRA) third party node
0 KKR&A)
wherein said Sad" encrypted with said KKR&A is utilized for decrypting said dynamic **public key** of said first node.

9 The message of claim 8, wherein said first node comprises...

...first node, PA", with a static private
key of said KRA device,
determining a static **common session key** , K!@MAA, between said KRA device
andsaidfirstnode,basedonsaidPA"andSKRA',
retrieving a first exchange message, EKmRxA...

...second node, (SBdyn(T)), based on
said EKOaL,,,B) (SB"yn(T)),
determining a dynamic **public key** of said second node, P,3"'(T), based on
2 0 said SBdyn(T), and
determining said dynamic **common key** , Kdy"XB(T), based on said SAdyn(T) and said PBdI', for decrypting messages transmitted...

18/5,K/29 (Item 29 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00372598 **Image available**
NETWORK SECURITY DEVICE
DISPOSITIF DE SECURITE DE RESEAU
Patent Applicant/Assignee:
DIGITAL SECURED NETWORKS TECHNOLOGY INC,
Inventor(s):
FRIEDMAN Aharon,
LEVY Ben Zion,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9713340 A1 19970410
Application: WO 96US14285 19960906 (PCT/WO US9614285)
Priority Application: US 95529497 19950918
Designated States: AL AM AU BB BG BR CA CN CU CZ EE FI GE HU IL IS JP KG KP KR LC LK LR LT LV MD MG MK MN MX NO NZ PL RO SG SI SK TR TT UA UZ VN KE LS MW SD SZ UG AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Main International Patent Class: H04L-009/00
International Patent Class: H04J-03:26
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6994

English Abstract
A network security device (10) is connected between a protected client (12) and a network (100). The network security device (10) negotiates a session key with any other protected client. Then, all communications between the two clients are encrypted. The inventive device is self-configuring and locks itself to the IP address of its client (12). Thus, the client (12) cannot change its IP address once set and therefore cannot emulate the IP address of another client. When a packet is transmitted from the protected host, the security device (10) translates the MAC address of the client to its own MAC address before transmitting the packet into the network. Packets addressed to the host, contain the MAC address of the security device. The security device (10) translates its MAC address to the client's (12) MAC address before transmitting the packet to the client (12).

French Abstract
L'invention a trait a un dispositif de securite de reseau (10) connecte entre un client protege (12) et un reseau (100). Ce dispositif (10) negocie une clef de session avec n'importe quel autre client protege. Toutes les communications entre les deux clients sont alors cryptees. Le dispositif selon l'invention s'auto-configure et verrouille de lui-meme l'adresse IP (Protocole Internet) de son client (12). De la sorte, ce dernier est dans l'impossibilite de modifier son adresse IP, une fois celle-ci arretee, et, partant, ne peut emuler l'adresse IP d'un autre client. Lorsque l'hote protege transmet un paquet, le dispositif de securite (10) transforme, en la traduisant, l'adresse MAC du client en sa propre adresse MAC avant d'envoyer le paquet sur le reseau. Les paquets adresses a l'hote contiennent l'adresse MAC du dispositif de securite. Celui-ci (10) transforme, en la traduisant, sa propre adresse MAC en adresse MAC du client (12) avant d'envoyer le paquet au client (12).

Fulltext Availability:
Claims

Claim
... in said network.

19 The method of claim 18 wherein said step of negotiating a **common session key** comprises the steps of (1) at said network security device, using a static **public key** of said second node, encrypting a dynamic 20 **public key** of said first node and transmitting said dynamic **public key** of said first node to said second node, (2) receiving from said second node a dynamic **public key** of said second node encrypted with a static **public key** of said first node and decrypting said dynamic **public key** of said second node with a static secret key of said f irst node at said network security device, (3) at said network security device, generating said **common session key** from a dynamic secret key of said first host and said dynamic **public key** of said second node.

20 The method of claim 19 wherein said first node maintains...
?